Alex Morris

The Dilemma of Digital Colonialism

unmasking facial recognition technology and data sovereignty in Aotearoa New Zealand

Abstract

Law enforcement agencies have become increasingly reliant upon facial recognition technology (FRT) as a powerful surveillance tool in the fight against crime. Developing at an unprecedented rate, FRT has exceeded the incremental pace of law and policy. This has resulted in unregulated over-surveillance, triggering questions about police misconduct and ethnic discrimination. In Aotearoa New Zealand, targeted surveillance and the emergence of FRT have reignited concerns over inherent colonialist practices, dismissive of obligations to te Tiriti o Waitangi and Māori rights. They have also provided for a new wave of discussion on how future policy might incorporate Māori data sovereignty. While a highly valuable policing tool, its lack of regulation, technological accuracy and potential racial bias have led some countries, including Aotearoa New Zealand, to impose a moratorium on FRT use in law enforcement. Policymakers must now look at how to dismantle what is fast becoming an age of digital colonialism.

Keywords facial recognition technology, Māori data sovereignty, surveillance, data colonialism, emerging technologies, law enforcement

Alex Morris is a researcher/analyst at the Waitangi Tribunal.

Facial recognition technology – 21st-century surveillance

Facial recognition technology in law enforcement

While surveillance in law enforcement is by no means a new phenomenon, facial recognition technology (FRT) has been touted as the gateway to innovations in smart policing (Bromberg, Charbonneau and Smith, 2020; Feldstein, 2021). FRT is a tool to compare, verify and confirm someone's identity. It relies on an FRT algorithm, conducting a biometric scan to extract a person's unique facial geometric features, such as the distance between the eyes, nose and mouth, and the structural composition of the forehead and cheekbones, to create the equivalent of a digital footprint (Lynch and Chen, 2021). These geometric features are then collated in the form of data and used to link individuals to pre-existing images stored on a database.

Automated (live) FRT is the newest and most controversial form of smart surveillance, as it can identify people in real time without their prior knowledge or consent. However, police maintain that its speed and efficiency have proven highly

effective in crime prevention and counterterrorism operations, able to detect people from a distance in large, fast-moving crowds. Internationally, law enforcement agencies have sought to expand FRT on the premise that it can increase public and police safety and security, promote de-escalation methods, and improve accountability and efficiency (Bragias, Heine and Fleet, 2021; Schwartz, 2017; Smith and Miller, 2021).

The threat to privacy

Until recently, police have been afforded unregulated discretion over FRT, testing the boundaries of privacy. Roberts et al. (2020) highlight how China has used FRT to closely monitor the moral behaviour of its citizens in a push for digital social governance. People have been 'blacklisted' for what the government considers 'immoral' behaviour and reprimanded through measures of public shaming and the removal of the right to privileges, such as purchasing first-class train tickets or sending children to prestigious schools. Furthermore, China is also utilising FRT as a tool to persecute and purge the minority Uyghur population, under the premise that they are a potential terrorist threat (ibid.; Van Noorden, 2020). During the Covid-19 pandemic Russia, China and Malaysia have merged thermal technology with FRT to locate people with high temperatures, monitor positive cases and detect quarantine-breakers (Lynch et al., 2020; Roussi, 2020). China has even adopted emotional FRT, which has the added capability of inferring people's feelings through analysing their facial expressions (Standaert, 2021). Yet concern is mounting that this cutting-edge technology feels somewhat akin to dystopian depictions of authoritarian surveillance regimes designed to restrict basic human rights rather than prevent crime and disorder.

The lack of FRT regulatory measures has also impacted how personal data is being collected and retained. In 2020, Clearview AI (a US-based company specialising in FRT) was exposed for harvesting over 3 billion personal data images, scraped from social media platforms such as Facebook, YouTube and Instagram (Hill, 2020a). The company had used these images in its identification application, which it then supplied to law enforcement agencies across the United States, Australia, the United Kingdom and New Zealand. Clearview AI was also retaining sensitive images collected by the police, unregulated and without public scrutiny (Lynch et al., 2020; Smith and Miller, 2021). The UK, France, Italy and Australia have since attempted to enforce more stringent data regulatory measures, discontinuing business with Clearview AI, ordering them to delete data and imposing fines for violating data protection laws. However, the company has refused to cooperate on the basis that it is not bound by EU and British jurisdictions. Since 2020 the size of Clearview AI's database has skyrocketed: it now holds a collection of over 20 billion facial images, which are globally available to all the company's clients (McCallum, 2022). Data scraping, data retention, and the sale of biometric information without active consent are a clear violation of privacy rights, regardless of whether the technology is used for law enforcement purposes or by private companies. While firms such as Clearview AI can blatantly flout jurisdiction and continue to use personal information, there remains an urgent need for more robust legislation and transnational cooperation.

> Currently, there is a tendency to compartmentalise the causes and effects of AI bias and attribute blame to individuals or technological malfunctions, rather than acknowledging bias as an ingrained societal construct ...

Bias and discrimination

Researchers have also warned against utilising FRT software prematurely, citing evidence of flawed and discriminatory FRT algorithmic systems (Lynch and Chen, 2021). While performing post-crime search and scan procedures manually through fixed CCTV footage is common in police practice, the replacement of manual identification with algorithms is relatively nuanced and a complex technological process. Algorithmic identification is inherently different from human analysis, as even minor changes in pixilation – unnoticeable to a human – may significantly affect the identification process, resulting in false positives (or false negatives) (Ruhrmann, 2019). In 2017, for example, the South Wales Police misidentified over 2,000 people when using automated FRT to monitor fans at the UEFA Champions League final; this was due to poor image quality and incomplete data sources (BBC, 2018; Fussey, Davies and McInnes, 2021).

In determining the cause of algorithmic error, scholars have highlighted that one explanation is underdeveloped training data sets, which algorithms rely on to identify facial images (Feldstein, 2021; Hoffmann, 2019; Zajko, 2021). Despite ongoing AI performance development, there is now substantial research showing that algorithmic error is contributing to the reproduction of ethnic and gender bias. This points to sounder FRT accuracy for white males compared with higher rates of false positives and false negatives for females and those with darker skin; darker-skinned females are thus significantly disadvantaged and more likely to suffer from bias (Buolamwini and Gebru, 2018; Grother, Ngan and Hanaoka, 2018). The US National Institute of Standards and Technology 2019 study on the demographic effects of FRT supports this hypothesis. Findings revealed that in the US, African Americans and Asians were 10–100 times more likely to produce false positive matches than other ethnicities, highlighting insufficient demographic diversity in data sets (Grother, Ngan and Hanaoka, 2019). If

used in law enforcement, FRT will likely depend on biased data and may result in unjust or inaccurate outcomes (Buolamwini and Gebru, 2018; Fussey and Murray, 2019). A prime example of this occurred in 2020 with the arrest of Robert Williams, an African American who was detained and interrogated for a shoplifting offence resulting from an FRT match which was later found to be a false positive (Hill, 2020b). While this is based on Western data sets – as opposed to data sets in China which have higher accuracy rates – it illustrates the detrimental impact of algorithmic discrepancies if data sets do not provide sufficient demographic representation.

Currently, there is a tendency to compartmentalise the causes and effects of AI bias and attribute blame to individuals or technological malfunctions, rather than acknowledging bias as an ingrained societal construct (Hoffmann, 2019). While designing fair and equitable AI systems is critical, this alone cannot eliminate bias and discrimination; it requires an intersectional approach to better understand how technology and colonialism are entwined (Buolamwini and Gebru, 2018; Hoffmann, 2019; Zajko, 2021). Furthermore, as Fussey, Davies and McInnes have observed, in law enforcement 'the rules encoded within the algorithms are not "unbending" and inflexible but configured and constructed via a range of policing influences' (Fussey, Davies and McInnes, 2021, p.342). Again, this points to data as a man-made construct. The reality is that humans and technology need to co-exist, with appropriate accountability mechanisms and the assurance that responsibility cannot be externalised at the convenience of the designer, politician, police, or anyone who finds themselves under fire for FRT's technical shortcomings. Essential to this process is the deconstruction of digital colonialism.

Indigenous rights to data sovereignty

FRT data collection and storage has further provoked questions over indigenous rights. The manipulation of data has long involved the control of indigenous minorities; from an indigenous perspective, combining surveillance technology with mass data collection is an inherently colonialist approach, suppressing the indigenous right to self-determination (Cormack, Kukutai and Cormack, 2020).

> While there has been a move towards improving data collection efficiency through New Zealand's Integrated Data Infrastructure (IDI) – a streamlined, cross-government data network – structures remain inherently Eurocentric.

In recent years there has been a drive to dismantle oppressive data constructs through recognising indigenous data sovereignty. Indigenous data sovereignty realises the rights of indigenous peoples to manage and govern their own data, based on alternative approaches to data governance and the appreciation of data as a living representation of culture, ancestry and history (ibid.; Hudson et al., 2017). Witnessed on an international scale, governments and politicians can no longer feign ignorance about the inadequacies of data management. In 2018 the special rapporteur for the United Nations released a report imploring member states to recognise indigenous data sovereignty. The report succinctly outlines the fragility of indigenous interests, stating:

> Indigenous peoples remain largely alienated from the collection, use and application of data about them, their lands and cultures. Existing data and data infrastructure fail to recognize or privilege indigenous knowledge and worldviews and do not meet indigenous peoples' current and future data needs. (Cannataci, 2018, p.13)

To date, indigenous data sovereignty has largely been absent from public policy. Kukutai and Cormack (2021) argue that indigenous data sovereignty can only be truly empowered through indigenous data governance. However, creating indigenous data ecosystems requires legislation and policy, rather than relying on voluntary charters and principles alone.

Digital colonialism in Aotearoa New Zealand

A history of surveillance

Aotearoa New Zealand has a long and fraught history of racial surveillance, discrimination, and a failure to develop policy which prevents bias (Norris and Tauri, 2021). This is bound in colonial policing practices, notorious for targeting Māori. Currently, while Māori comprise only 16.5% of New Zealand's population, they make up 56% of the prison population (Department of Corrections, 2022). The explanations behind the disproportionate incarceration rates have been widely debated among scholars, citing reasons such as socio-economic and intergenerational disadvantages, embedded structural racism, and a power imbalance between Māori and the Crown (McIntosh and Workman, 2017; Norris and Tauri, 2021; Webb, 2017). Many argue that colonisation and colonial practices remain the underlying cause, not only of repeat offending and high imprisonment rates, but also of systemic bias; this in turn has fuelled a lack of faith in policing practices (Stanley and Bradley, 2021).

In 2020 it was disclosed that the New Zealand Police had been photographing Māori and Pasifika on a targeted basis. Police had photographed rangatahi Māori without cause or consent, retaining their data on the national police database (NIA)

as 'intel notings' (Hurihanganui and Cardwell, 2020; Hurihanganui, 2021). Following a joint inquiry into police behaviour, the Independent Police Conduct Authority (IPCA) and the Office of the Privacy Commissioner found that since 2018, 45% of photographs attached to intel notings on the NIA database were of Māori and 10% were of Pasifika (Independent Police Conduct Authority and Office of the Privacy Commissioner, 2022). Other issues included the lack of policy on storing photographs on police mobile devices; retention of duplicate photographs; and breaches of the Privacy Act 1993 and the Oranga Tamariki Act through unlawful photographs taken of rangatahi Māori. This again raises questions of racial profiling and existing gaps in legislation which allow for the collection and retention of data.

The future of surveillance policy

In December 2021 the New Zealand Police announced the suspension of automated FRT in response to an independent report, carried out following the growing national unrest over its controversial use. The report contended that without a better understanding of the legal, privacy and ethical impacts, FRT could be detrimental to social licence (Lynch and Chen, 2021). Mark Evans, deputy chief inspector of the New Zealand Police, announced that the suspension was an opportunity to 'prepare for any considered future adoption of the technology' (New Zealand Police, 2021). This included a commitment to community engagement, addressing concerns related to FRT bias, and approaching its use in a safe and responsible manner.

Since then, the New Zealand Police have thankfully demonstrated a considerably more transparent and proactive approach. In July 2022 an updated policy on emerging technologies was published (New Zealand Police, 2022b). The policy captures both new and well-established technologies with either new capabilities or improved functionalities that change the purpose of their use; this includes FRT, machine learning, AI, drones and CCTV. The primary objectives are to enhance accountability and transparency, dispelling public mistrust over surveillance. The police have also since published a 'New Technology Framework', which sets out ten principles for consideration when adopting a new technology. Another positive sign is the acknowledgment of data sovereignty in principle 4 of the framework, which states: 'If the technology includes any form of data collection and use, relevant mechanisms are in place to ensure data is treated as taonga and Māori sovereignty is maintained' (New Zealand Police, 2022a, p.8).

> The [Integrated Data Infrastructure] has neglected to consider te ao Māori data values and principles, continuing to store data offshore and diminishing the Māori right to tino rangatiratanga ...

While both the policy and framework acknowledge police obligations under te Tiriti o Waitangi, taking account of a te ao Māori perspective, and the importance of partnership, they fail to detail how, practically, this will be achieved. The framework only provides broad guidance on how the policy and principles should be applied. For instance, *how* should te ao Māori be considered? Which relevant mechanisms will ensure data is treated as taonga? Although the moratorium on FRT remains in place, it is unlikely that this will become permanent, given FRT's vast scope as a policing tool. As things stand, the efficacy of this policy in practice – particularly regarding the practical measures taken to avoid future injustices and privacy violations – is yet to be determined.

The emergence of Māori data sovereignty

While there has been a move towards improving data collection efficiency through New Zealand's Integrated Data Infrastructure (IDI) – a streamlined, cross-government data network – structures remain inherently Eurocentric. The IDI has neglected to consider te ao Māori data values and principles, continuing to store data offshore and diminishing the Māori right to tino rangatiratanga (Kukutai and Cormack, 2019; Moses, 2020). Its rapid expansion has also led to procedural gaps, such as a lack of Māori inclusion and consultation, the failure to gain consent to reuse data as a secondary means, and the absence of policy (Sporle, Hudson and West, 2021). There is also evidence that policymakers have become too reliant on algorithms, integrated data sets and predictive statistical modelling to draw conclusions about population needs and social investment (Kukutai and Cormack, 2019). Moses (2020) argues that these practices have neglected to fully account for the disproportionate representation and over-surveillance of Māori.

Emerging from indigenous data sovereignty, the concept of Māori data sovereignty has gained significant traction in Aotearoa New Zealand. Based on mātauranga Māori ontologies of collectivism and relativism, Māori data sovereignty illustrates another layer of tino rangatiratanga, neglected due to Eurocentric domains of governance. Māori data sovereignty considers data as a taonga, giving Māori the right to governance under article 2 of te Tiriti o Waitangi (Te Mana Raraunga, 2021). Data should be treated according to tikanga-based values such as wellbeing and restoration, encouraging manaakitanga and kaitiakitanga (Cormack, Kukutai and Cormack, 2020).

Established in 2016, Te Mana Raraunga (the Māori Data Sovereignty Network) has led the drive for an alternative view of data management, pooling the knowledge of Māori scholars, researchers and practitioners to foster a better

understanding of Māori data sovereignty and protect Māori rights on a national level. In its charter, Te Mana Raraunga states that:

- Data is a living taonga and is of strategic value to Māori.
- Māori data refers to data produced by Māori or that is about Māori and the environments we have relationships with. (Te Mana Raraunga, 2021, p.1)

Working in tandem with the National Iwi Chairs Forum's Data Iwi Leadership Group, Te Mana Raraunga has advocated for an ethical approach to data through the mana-mahi framework set out in the charter. It presents an approach based on six principles – whanaungatanga, rangatiratanga, kotahitanga, manaakitanga and kaitiakitanga. Together, these principles form the basis for a future in which Māori data rights are respected and valued. However, a caveat to this approach concerns determining whether data is a taonga and therefore subject to article 2 of te Tiriti. The Waitangi Tribunal (2021) acknowledged that Māori data has the potential to be a taonga as part of mātauranga Māori, but could not conclude whether all data was a taonga. Certain scholars have concluded that this must be deduced on a contextual basis (Dewes, 2017; Hudson et al., 2017). Developing a comprehensive assessment process in partnership with Māori to determine whether data is a taonga will be key to the future of data sovereignty across not only police policy, but all realms of governance.

Māori data sovereignty in policymaking

While concrete policy is yet to materialise, the language of Māori data sovereignty is beginning to appear in policy documentation, and various agencies and government departments have expressed interest in incorporating Māori data sovereignty principles into practice (Sporle, Hudson and West, 2021). StatsNZ has committed to forging a better relationship with Māori through the signing of a Mana Ōrite Relationship Agreement, pledging partnership and focusing on a future data network of co-design and co-creation with Māori (StatsNZ, 2021).

In 2020 the New Zealand Police, along with other government agencies, signed the Algorithm Charter for Aotearoa New Zealand, committing to safeguarding privacy and ethics, managing bias, and embedding a te ao Māori perspective in the use of algorithms (New Zealand Government, 2020). However, apart from StatsNZ's Mana Ōrite agreement, there are no other frameworks pertaining to the ethical use of data that include Māori as a partner in data management. While the algorithm charter pledges commitment to incorporating a te ao Māori perspective, it states that it is unable to 'fully address' Māori data sovereignty. The current system remains built upon Western capitalist assumptions, such as individual privacy and property rights, and remains incompatible with Māori data sovereignty approaches. While it would, of course, be a momentous challenge, there is an opportunity for policymakers to deconstruct colonial data management and redesign it from the ground up.

The inclusion of Māori data sovereignty in policy may require the establishment of a consistent cross-government framework to determine whether data is a taonga and to move towards alternative methods of data management.

What happens next?

The development of a new policy and framework for emerging technologies is a promising start in terms of policing and this new frontier may well transpire into further scope for robust Māori–Crown relations. On the other hand, if concrete actions remain wanting, it may simply cement the longstanding criticism of an unwillingness to relinquish the colonialist reins. Below we discuss in brief how the police could further solidify their commitment to improving FRT regulations and data use in Aotearoa New Zealand.

A data sovereignty assessment framework

The inclusion of Māori data sovereignty in policy may require the establishment of a consistent cross-government framework to determine whether data is a taonga and to move towards alternative methods of data management. Any such framework would need to analyse whether the data has been obtained by consent and whether is it being utilised as a secondary source. In a similar vein to the secondary use of data held in the IDI, police have retained and reused facial images without consent. Data collection and retention where there has been no probable cause is particularly questionable. If this method of data collection is re-established in the future – particularly in terms of FRT – it is critical to maintain transparency regarding how Māori will be affected; currently, there are only internal police mechanisms in place to ascertain whether data is being used ethically or whether it is being misappropriated.

Moving towards data ecosystems which allow Māori authority over their data and are shaped by tikanga may be one solution to creating an ethical, Tiriti-based approach to data management (Kukutai and Cormack, 2021). This would involve establishing a fair and transparent process to determine an appropriate degree of autonomy. Hudson et al. (2017) suggest that the level of authority Māori are afforded over data control is largely dependent on the context and sensitivity of the data. If the data is of high sensitivity, then Māori should be entitled to greater control and equal decision-making rights; if it is data of moderate sensitivity, Māori

may only require consultation; if the data is of a less sensitive nature, it may qualify for public availability. How this may fare in terms of criminal justice data leads to discussion around Aotearoa New Zealand's current data legislation.

Legislation

It is important to acknowledge the absence of sufficient legislation relating to data management and privacy rights. While it has been established that indigenous peoples possess the right to self-determination and data sovereignty (Cannataci, 2018; United Nations, 2008), the circumstances under which those rights can be overruled remain unclear, particularly in terms of law enforcement. As was highlighted in the IPCA report, despite certain provisions for the protection of personal information set out in the Privacy Act, there are exceptions which allow the police to gather intelligence without obtaining consent or informing the individual (Independent Police Conduct Authority and Office of the Privacy Commissioner, 2022). As principles-based legislation, the Privacy Act provides flexibility, blurring the boundaries of what constitutes lawful collection and retention of personal information. While the Office of the Privacy Commissioner and IPCA have recommended that the New Zealand Police engage in further policy development and provide clearer guidelines for gathering intelligence, including the lawful collection and retention of photographs, the efficacy of such policies is yet to be determined. Further, the effectiveness of existing legislation in terms of protecting Māori data rights is tenuous to say the least: the Māori population remains over-represented in data sets and thus continues to suffer from bias (Cunneen and Tauri, 2016; Moses, 2020). Police have been allowed undue discretion over managing personal information, revealing a lax approach to upholding the right to privacy and failing to address inequitable practices such as targeted surveillance.

.. there is an opportunity to harness technologies such as facial recognition technology so that both the police and the public may benefit, while eliminating aggressive and invasive surveillance practices.

Data localisation

Finally, further consideration needs to be given to data storage. Part of embedding a te ao Māori approach involves seeing data from an alternative perspective, and in the case of Māori data sovereignty would involve a commitment to storing data locally (Cormack, Kukutai and Cormack, 2020). Storing data offshore poses a serious threat to data sovereignty, with the further loss of Māori control, inconsistent and insufficient data regulations, and lower accuracy rates, which has a detrimental effect on minority populations (Lynch and Chen, 2021). In committing to a fully nationalised data storage facility, Aotearoa New Zealand would both shore up security and better align with Māori data sovereignty values. Co-designing any such facility would be another positive step towards giving effect to tino rangatiratanga.

Conclusion

The repercussions of over-surveillance and ethnic discrimination have been witnessed on a global scale as law enforcement agencies have seized the opportunity to utilise digital surveillance to the detriment of human rights and privacy. However, there is an opportunity to harness technologies such as facial recognition technology so that both the police and the public may benefit, while eliminating aggressive and invasive surveillance practices. Each nation must look to this as the opportunity to be inclusive of indigenous populations, removing any threat of discriminatory practices, including both algorithmic and systemic biases.

Looking forward, not only should Aotearoa New Zealand's FRT policy include evidence of the steps required to actively ensure partnership with Māori; it should also demonstrate how this will remain a constant in the long term. Social licence has waned due to discriminatory targeted surveillance, but it is not the technology alone that is the cause. Policing systems have failed to keep pace with both the regulation of technologies and with the evolution of data management, lacking any insight into the harm caused by embedding colonialist data practices.

Implementing ethical, te ao Māori-based data collection and management systems will ensure that New Zealand Police policy aligns with te Tiriti o Waitangi and its principles. Māori data sovereignty represents the potential to dismantle data colonialism and transform how data is perceived. While this would challenge the very fabric of the capitalist-based information age, it would create the opportunity to eliminate digital colonialism and unethical practices such as unconsented data collection and retention. Furthermore, enforcing data localisation would strengthen not only Māori rangatiratanga, but also national control over data management. This provides both policymakers and the police with the unique opportunity to enhance partnership with Māori and approach emerging technology through a fair and just lens.

References

BBC (2018) '2000 wrongly matched with potential criminals at Champions League', BBC, 4 May, https://www.bbc.com/news/uk-wales-south-west-wales-44007872

Bragias, A., K. Hine and R. Fleet (2021) 'Only in our best interest, right? Public perceptions of police use of facial recognition technology', *Police Practice and Research*, 22 (6), pp.1637–54, https://doi.org/10.1080/15614263.2021.1942873

Bromberg, D.E., E. Charbonneau and A. Smith (2020) 'Public support for facial recognition via police body-worn cameras: findings from a list experiment', *Government Information Quarterly*, 37 (1), pp.1–8, https://doi.org/10.1016/j.giq.2019.101415

Buolamwini, J. and T. Gebru (2018) 'Gender shades: intersectional accuracy disparities in commercial gender classification', *PMLR*, 81, pp.77–91, http://proceedings.mlr.press/v81/buolamwini18a.html

Cannataci, J. (2018) *Report of the Special Rapporteur on the Right to Privacy A/73/438*, Office of the High Commissioner for Human Rights, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/324/46/PDF/N1832446.pdf?OpenElement

Cormack, D., T. Kukutai and C. Cormack (2020) 'Not one byte more: from data colonialism to data sovereignty', in A. Chen (ed.), *Shouting Zeros and Ones: digital technology ethics and policy in New Zealand*, Wellington: Bridget Williams Books

Cunneen, C. and J. Tauri (2016) *Indigenous Criminology*, Bristol: Policy Press

Department of Corrections (2022) 'Prison facts and statistics – September 2022', https://www.corrections.govt.nz/resources/statistics/quarterly_prison_statistics/prison_stats_september_2022

Dewes, T.K. (2017) '"He taonga ranei tēnei mea te raraunga": how is data a taonga?', report submitted for MAOR 591, University of Waikato

Feldstein, S. (2021) *The Rise of Digital Repression: how technology is reshaping power, politics, and resistance*, Oxford: Oxford University Press, https://doi.org/10.1093/oso/9780190057497.001.0001

Fussey, P., B. Davies and M. Innes (2021) '"Assisted" facial recognition and the reinvention of suspicion and discretion in digital policing', B*ritish Journal of Criminology*, 61 (2), pp.325–44, https://doi-org.ezproxy.auckland.ac.nz/10.1093/bjc/azaa068

Fussey, P. and D. Murray (2019) *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

Grother, P., M. Ngan and K. Hanaoka (2018) *Ongoing Face Recognition Vendor Test (FRVT): part 2 identification*, US Department of Commerce, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8238

Grother, P., M. Ngan and K. Hanaoka (2019) *Ongoing Face Recognition Vendor Test (FRVT): part 3 demographic effects*, US Department of Commerce, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8280

Hill, K. (2020a) 'The secretive company that might end privacy as we know it', *New York Times*, 18 January, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hill, K. (2020b) 'Wrongfully accused by an algorithm', *New York Times*, 3 August, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Hoffmann, A. (2019) 'Where fairness fails: data, algorithms, and the limits of antidiscrimination discourse', *Information, Communication and Society*, 22 (7), pp.900–15, http://doi.org/10.1080/1369118X.2019.1573912

Hudson, M., T. Anderson, T.K. Dewes, P. Temara, H. Whaanga and T. Roa (2017) '"He matapihi ki te mana raraunga": conceptualising big data through a Māori lens', in H. Whaanga, T. Keegan and M. Apperley (eds), *He Whare Hangarau Māori: language, culture and technology*, Hamilton: University of Waikato

Hurihanganui, T.A. (2021) 'Police using app to photograph innocent youth: "It's so wrong"', RNZ, 26 March, https://www.rnz.co.nz/news/in-depth/437944/police-using-app-to-photograph-innocent-youth-it-s-so-wrong

Hurihanganui, T.A. and H. Cardwell (2020) 'Questions raised after police officers stop youths to take their photos', RNZ, 21 December, https://www.rnz.co.nz/news/national/433285/questions-raised-after-police-officers-stop-youths-to-take-their-photos

Independent Police Complaints Authority and Office of the Privacy Commissioner (2022) 'Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into police conduct when photographing members of the public', https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Commissioner-inquiries/8-SEPTEMBER-2022-IPCA-AND-OPC-Joint-Inquiry-into-Police-photographing-of-members-of-the-public.pdf

Kukutai, T. and D. Cormack (2019) 'Mana motuhake ā-raraunga: datafication and social science research in Aotearoa', *New Zealand Journal of Social Sciences Online*, 14 (2), pp.201–8, https://doi.org/10.1080/1177083X.2019.1648304

Kukutai, T. and D. Cormack (2021) 'Pushing the space: data sovereignty and self-determination in Aotearoa NZ', in M. Walter, T. Kukutai, S.R. Carroll and D. Rodriguez-Lonebear (eds), *Indigenous Data Sovereignty and Policy*, London: Routledge, https://doi.org/10.4324/9780429273957

Lynch, N., L. Campbell, J. Purshouse and M. Betkier (2020) *Facial Recognition Technology in New Zealand: towards a legal and ethical framework*, Wellington: New Zealand Law Foundation, https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1913248/Facial-Recognition-Technology-in-NZ.pdf

Lynch, N. and A. Chen (2021) 'Facial recognition technology: considerations for use in policing', report commissioned by the New Zealand Police, https://www.police.govt.nz/sites/default/files/publications/facial-recognition-technology-considerations-for-use-policing.pdf

McCallum, S. (2022) 'Clearview AI fined in UK for illegally storing facial images', BBC, 23 May, https://www.bbc.com/news/technology-61550776

McIntosh, T. and K. Workman (2017) 'Māori and prison', in A. Deckert and R. Sarre (eds), *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*, London: Palgrave MacMillan, http://doi.org/10.1007/978-3-319-55747-2_48

Moses, C. (2020) 'The Integrated Data Infrastructure', in A. Chen (ed.), *Shouting Zeros and Ones: digital technology ethics and policy in New Zealand*, Wellington: Bridget Williams Books

New Zealand Government (2020) 'Algorithm Charter for Aotearoa New Zealand', https://www.police.govt.nz/sites/default/files/publications/algorithm-charter-english.pdf

New Zealand Police (2021) 'Police release findings from independent expert review of facial recognition technology', 9 December, https://www.police.govt.nz/news/release/police-release-findings-independent-expert-review-facial-recognition-technology

New Zealand Police (2022a) 'New technology framework', https://www.police.govt.nz/sites/default/files/publications/new-technology-framework.pdf

New Zealand Police (2022b) 'Trial or adoption of new emerging technology', https://www.police.govt.nz/sites/default/files/publications/trial-or-adoption-new-policing-technology-130722.pdf

Norris, A. and J. Tauri (2021) 'Racialized surveillance in New Zealand: from the Tūhoe raids to the extralegal photographing of indigenous youth', *Race and Justice*, 1 (1), pp.1–19, https://doi-org.ezproxy.auckland.ac.nz/10.1177/21533687211063581

Roberts, H., J. Cowls, J. Morley, M. Taddeo, V. Wang and L. Floridi (2020) 'The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation', *AI and Society*, 36 (1), pp.59–77, https://doi.org/10.1007/s00146-020-00992-2

Roussi, A. (2020) 'Resisting the rise of facial recognition', *Nature*, 587 (7834), pp.350–3, http://dx.doi.org/10.1038/d41586-020-03188-2

Ruhrmann, H. (2019) *Facing the Future: protecting human rights in policy strategies for facial recognition technology in law enforcement*, CITRIS Policy Lab, http://doi.org/10.13140/RG.2.2.22299.28967

Schwartz, S.C. (2017) 'Big brother or trusted allies? How the police can earn community support for using unmanned aircraft', MA thesis, Naval Postgraduate School, https://www.hsaj.org/articles/14437

Smith, M. (2020) 'Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI', RNZ, 15 May, https://www.rnz.co.nz/news/national/416697/police-searched-for-suspects-in-unapproved-trial-of-facial-recognition-tech-clearview-ai

Smith, M. and S. Miller (2021) 'The ethical application of biometric facial recognition technology', *AI and Society*, 37 (1), pp.167–75, https://doi-org.ezproxy.auckland.ac.nz/10.1007/s00146-021-01199-9

Sporle, A., M. Hudson and K. West (2021) 'Indigenous data and policy in Aotearoa New Zealand', in M. Walter, T. Kukutai, S.R. Carroll and D. Rodriguez-Lonebear (eds), *Indigenous Data Sovereignty and Policy*, London: Routledge, https://doi.org/10.4324/9780429273957

Standaert, M. (2021) 'Smile for the camera: the dark side of China's emotion-recognition tech', *Guardian*, 3 March, https://www.theguardian.com/global-development/2021/mar/03/china-positive-energy-emotion-surveillance-recognition-tech

Stanley, E. and T. Bradley (2021) 'Rethinking policing in Aotearoa New Zealand: decolonising lessons from the Covid-19 pandemic', *Criminal Justice*, 33 (1), pp.131–7, https://doi.org/10.1080/10345329.2020.1850145

StatsNZ (2021) 'Mana Ōrite Relationship Agreement', https://stats.govt.nz/about-us/what-we-do/mana-orite-relationship-agreement/

Te Mana Raraunga (2021) 'Māori data sovereignty network charter', https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/5913020d15cf7dde1df34482/1494417935052/Te+Mana+Raraunga+Charter+%28Final+%26+Approved%29.pdf

United Nations (2008) 'United Nations Declaration on the Rights of Indigenous Peoples', https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf

Van Noorden, R. (2020) 'The ethical questions that haunt facial recognition research', *Nature*, 587 (7834), pp.354–58, http://dx.doi.org/10.1038/d41586-020-03187-3

Waitangi Tribunal (2021) *The Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership*, WAI 2522, prepublication copy, https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_178856069/CPTTP%20W.pdf

Webb, R. (2017) 'Māori experiences of colonisation and criminology', in A. Deckert and R. Sarre (eds), *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*, London: Palgrave MacMillan, http://doi.org/10.1007/978-3-319-55747-2_45

Zajko, M. (2021) 'Conservative AI and social inequality: conceptualizing alternatives to bias through social theory', *AI and Society*, 36, pp.1047–56, https://link-springer-com.ezproxy.auckland.ac.nz/article/10.1007/s00146-021-01153-9